Queen Mary
University of London

C50 Enumerative & Asymptotic Combinatorics

Notes 2 **Spring 2003**

In this section we do some counting related to the fundamental objects of combinatorics: subsets, partitions, and permutations. The counting functions have two parameters: n, the size of the underlying set; and k, a measure of the object in question (the number of elements of a subset, parts of a partition, or cycles of a permutation respectively).

Subsets

The number of k-element subsets of the set $\{1,\ldots,n\}$ is the *binomial coefficient*

$$\binom{n}{k} = \begin{cases} 0 & \text{if } k<0 \text{ or } k>n; \\ \dfrac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1} & \text{if } 0\le k\le n. \end{cases}$$

For, if $0\le k\le n$, there are $n(n-1)\cdots(n-k)$ ways to choose in order k distinct elements from $\{1,\ldots,n\}$; each k-element subset is obtained from $k!$ such ordered selections. The result for $k<0$ or $k>n$ is clear.

Proposition 1 *The recurrence relation for the binomial coefficients is*

$$\binom{n}{0} = \binom{n}{n} = 1, \qquad \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \text{ for } 0<k<n.$$

Proof Partition the k-element subsets into two classes: those containing n (which have the form $\{n\}\cup L$, where L is a $(k-1)$-element subset of $\{1,\ldots,n-1\}$, and so are $\binom{n-1}{k-1}$ in number); and those not containing n (which are k-element subsets of $\{1,\ldots,n-1\}$, and so are $\binom{n-1}{k}$ in number).

The *binomial theorem* for natural number exponents n asserts:

Proposition 2 $(x+y)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k.$

Proof The proof is straightforward. On the left we have the product

$$(x+y)(x+y)\cdots(x+y) \qquad (n \text{ factors});$$

multiplying this out we get the sum of 2^n terms, each of which is obtained by choosing y from a subset of the factors and x from the remainder. There are $\binom{n}{k}$ subsets of size k, and each contributes a term $x^{n-k}y^k$ to the sum, for $k = 0, \ldots, n$.

The Binomial Theorem can be looked at in various ways. From one point of view, it gives the generating function for the binomial coefficients $\binom{n}{k}$ for fixed n:

$$\sum_{k\geq 0} \binom{n}{k} y^k = (1+y)^n.$$

Since the binomial coefficients have two indices, we could ask for a two-variable generating function:

$$\begin{aligned} \sum_{n\geq 0}\sum_{k\geq 0} \binom{n}{k} x^n y^k &= \sum_{n\geq 0} x^n (1+y)^n \\ &= \frac{1}{1-x(1+y)}. \end{aligned}$$

If we expand this in powers of y, we obtain

$$\begin{aligned} \frac{1}{(1-x)-xy} &= \frac{1}{1-x} \cdot \frac{1}{1-(x/(1-x))y} \\ &= \sum_{k\geq 0} \left(\frac{x^k}{(1-x)^{k+1}} \right) y^k, \end{aligned}$$

so that we have the following:

Proposition 3 $\displaystyle\sum_{n\geq k} \binom{n}{k} x^n = \frac{x^k}{(1-x)^{k+1}}.$

Our next observation on the Binomial Theorem concerns *Pascal's Triangle*, the triangle whose nth row contains the numbers $\binom{n}{k}$ for $0 \leq k \leq n$. (Despite the name, this triangle was not invented by Pascal but occurs in earlier Chinese sources. Figure 1 shows the triangle as given in Chu Shi-Chieh's *Ssu Yuan Yü Chien*, dated 1303.) The recurrence relation shows that each entry of the triangle is the sum of the two above it.

At risk of making the triangle asymmetric, we turn it into a matrix $B = (b_{nk})$, where $b_{nk} = \binom{n}{k}$ for $n, k \geq 0$. This infinite matrix is lower triangular, with ones on the

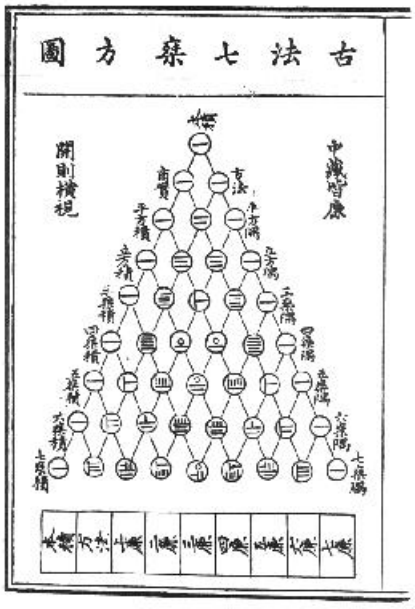

Figure 1: Chu Shi-Chieh's Triangle

diagonal. Now when two lower triangular matrices are multiplied, each term of the product is only a finite sum: the (n,k) entry of BC is $\sum_m b_{nm}c_{mk}$, and this is non-zero only for $k \leq m \leq n$. In particular, we can ask "What is the inverse of B?"

The *signed matrix of binomial coefficients* is the matrix B^* with (n,k) entry $(-1)^{n-k}\binom{n}{k}$. That is, it is the same as B except that signs of alternate terms are changed in a chess-board pattern. Now:

Proposition 4 *The inverse of the matrix B of binomial coefficients is the matrix B^* of signed binomial coefficients.*

Proof We consider the vector space of polynomials (over $\mathbb{R}$). There is a natural basis consisting of the polynomials $1, x, x^2, \ldots$. Now, since

$$(1+x)^n = \sum_k \binom{n}{k} x^k,$$

we see that B represents the change of basis to $1, y, y^2, \ldots$, where $y = 1+x$. Hence the inverse of B represents the basis change in the other direction, given by $x = y-1$. Since

$$(y-1)^n = \sum_k (-1)^{n-k} \binom{n}{k} y^k,$$

the matrix of this basis change is B^*.

The other aspect of the Binomial Theorem is its generalisation to arbitrary real exponents (due to Isaac Newton). This depends on a revised definition of the binomial coefficients.

Let a be an arbitrary real (or complex) number, and k a non-negative integer. Define

$$\binom{a}{k} = \frac{a(a-1)\cdots(a-k+1)}{k!}.$$

Note that this agrees with the previous definition in the case when n is a non-negative integer, since if $k > n$ then one of the factors in the numerator is zero. We do not define this version of the binomial coefficients if k is not a natural number.

Now the *binomial theorem* asserts that, for any real number a, we have

$$(1+x)^a = \sum_{k\geq 0} \binom{a}{k} x^k. \tag{1}$$

Is this a theorem or a definition? If we regard it as an equation connecting real functions (where the left-hand side is defined by

$$(1+x)^a = \exp(a\log(1+x)), \tag{2}$$

and the series on the right-hand side is convergent for $|x| < 1$), it is a theorem, and was understood by Newton in this form. As an equation connecting formal power series, we may follow the same approach, or we may instead choose to regard (1) as the definition and (2) as the theorem, according to taste. Whichever approach we take, we need to know that the laws of exponents hold:

$$\begin{aligned} (1+x)^a \cdot (1+y)^a &= (1+(x+y+xy))^a, \\ (1+x)^{a+b} &= (1+x)^a \cdot (1+x)^b, \\ (1+x)^{ab} &= ((1+x)^a)^b. \end{aligned}$$

If (1) is our definition, these verifications will reduce to identities between binomial coefficients; if (2) is the definition, they depend on properties of the power series for exp and log, defined as in the last chapter.

Binomial coefficients can be estimated by using Stirling's formula. For example, if n is even,

$$\binom{n}{n/2} \sim \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n \Big/ \pi n\left(\frac{n}{2\mathrm{e}}\right)^n = \frac{2^n}{\sqrt{\pi n/2}}.$$

The *central limit theorem* from probability theory can also be used to get estimates for binomial coeffients. Suppose that a fair coin is tossed n times. Then the probability of obtaining k heads is equal to $\binom{n}{k}/2^n$. Now the number of heads is a binomial random variable X; so we have

$$\mathbb{P}(X = k) = \binom{n}{k} \Big/ 2^n. \tag{3}$$

According to the Central Limit Theorem, if n is large then X is approximated by a normal random variable Y with the same expected value $n/2$ and variance $n/4$. The probability density function of Y is given by

$$f_Y(y) = \frac{1}{\sqrt{\pi n/2}} \mathrm{e}^{2(k-n/2)^2/n}. \tag{4}$$

If $k = n/2 + O(\sqrt{n})$ and $n \to \infty$, then a precise statement of the Central Limit Theorem shows that (4) gives an asymptotic formula for (3). In particular, when $k = n/2$, we obtain the preceding result. (You might like to check that the constant in Stirling's formula can be deduced from the Central Limit Theorem in this way.

Partitions

The *Bell number* $B(n)$ is the number of partitions of the set $\{1,\ldots,n\}$. There is a related "unlabelled" counting number $p(n)$, the *partition number*, which is the number of partitions of the number n (that is, lists in non-increasing order of positive integers with sum n). Thus, given any set partition, the list of sizes of its parts is a number partition; and two set partitions are equivalent under relabelling the elements of the underlying set (that is, under permutations of $\{1,\ldots,n\}$) if and only if the corresponding number partitions are equal.

What would be the analogous "unlabelled" counting function for subsets? Two subsets of $\{1,\ldots,n\}$ are equivalent under permutations if and only if they have the same cardinality; so the unlabelled counting function f for subsets would be simply $f(n) = n+1$.

Set partitions

The *Stirling numbers of the second kind*, denoted by $S(n,k)$, are defined by the rule that $S(n,k)$ is the number of partitions of $\{1,\ldots,n\}$ into k parts if $1 \le n \le k$, and zero otherwise. Clearly we have

$$\sum_{k=1}^{n} S(n,k) = B(n),$$

where the Bell number $B(n)$ is the total number of partitions of $\{1,\ldots,n\}$.

Proposition 5 *The recurrence relation for the Stirling numbers is*

$$S(n,1) = S(n,n) = 1, \qquad S(n,k) = S(n-1,k-1) + kS(n-1,k) \text{ for } 1 < k < n.$$

Proof We split the partitions into two classes: those for which $\{n\}$ is a single part (obtained by adjoining this part to a partition of $\{1,\ldots,n-1\}$ into $k-1$ parts), and the remainder (obtained by taking a partition of $\{1,\ldots,n-1\}$ into k parts, selecting one part, and adding n to it).

Proposition 6 *(a) The Stirling numbers satisfy the recurrence*

$$S(n,k) = \sum_{i=1}^{n-1} \binom{n-1}{i-1} S(n-i,k-1).$$

(b) The Bell numbers saisfy the recurrence

$$B(n) = \sum_{i=1}^{n} \binom{n-1}{i-1} B(n-i).$$

Proof Consider the part containing n of an arbitrary partition with k parts; suppose that it has cardinality i. Then there are $\binom{n-1}{k-1}$ choices for the remaining $i-1$ elements in this part, and $S(n-i,k-1)$ partitions of the remaining $n-i$ elements into $k-1$ parts. This proves (a); the proof of (b) is almost identical.

The Stirling numbers also have the following property. Let $(x)_k$ denote the polynomial $x(x-1)\cdots(x-k+1)$.

Proposition 7 $x^n = \sum_{k=1}^{n} S(n,k)(x)_k$.

Proof We prove this first when x is a positive integer. We take a set X with x elements, and count the number of n-tuples of elements of x. The total number is of course x^n. We now count them another way. Given an n-tuple $(x_1,\ldots,x_n)$, we define an equivalence relation on $\{1,\ldots,n\}$ by $i \equiv j$ if and only if $x_i = x_j$. If this relation has k different classes, then there are k distinct elements among $x_1,\ldots,x_n$, say $y_1,\ldots,y_k$ (listed in order). The choice of the partition and the k-tuple $(y_1,\ldots,y_k)$ uniquely determines $(x_1,\ldots,x_n)$. So the number of n-tuples is given by the right-hand expression also.

Now this equation between two polynomials of degree n holds for any positive integer x, so it must be a polynomial identity.

Stirling numbers are involved in the substitution of $\exp(x)-1$ for x in formal power series. The result depends on the following lemma:

Lemma 8

$$\sum_{n\geq k}\frac{S(n,k)x^n}{n!}=\frac{(\exp(x)-1)^k}{k!}.$$

Proof The proof is by induction on k, the result being true when $k=1$ since $S(n,1)=1$. Suppose that it holds when $k=l-1$. Then (setting $S(n,k)=0$ if $n<k$) we have

$$\begin{aligned}\frac{(\exp(x)-1)^l}{l!} &= \frac{1}{l}\cdot(\exp(x)-1)\cdot\frac{(\exp(x)-1)^{l-1}}{(l-1)!}\\ &= \frac{1}{l}\left(\sum_{n\geq 1}\frac{x^n}{n!}\right)\cdot\left(\sum_{n\geq 1}\frac{S(n,l-1)x^n}{n!}\right).\end{aligned}$$

The coefficient of $x^n/n!$ here is

$$\begin{aligned}\frac{n!}{l}\sum_{i=1}^{n-1}\frac{1}{i!}\cdot\frac{S(n-i,l-1)}{(n-i)!} &= \frac{1}{l}\sum_{i=1}^{n-1}\binom{n}{i}S(n-i,l-1)\\ &= \frac{1}{l}(S(n+1,l)-S(n,l-1)),\end{aligned}$$

using the recurrence relation of Proposition 6(a). Finally, the recurrence relation of Proposition 5 shows that this is $S(n,l)$, as required.

Proposition 9 *Let $(a_0,a_1,\ldots)$ and $(b_0,b_1,\ldots)$ be two sequences of numbers, with exponential generating functions $A(x)$ and $B(x)$ respectively. Then the following two conditions are equivalent:*

(a) $b_0=a_0$ and $b_n=\sum_{k=1}^n S(n,k)a_k$ for $n\geq 1$;

(b) $B(x)=A(\exp(x)-1)$.

Proof Suppose that (a) holds. Without loss of generality we may assume that $a_0=b_0=0$. Then

$$B(x) = \sum_{n\geq 1}\frac{b_n x^n}{n!}$$

$$\begin{aligned} &= \sum_{n\geq 1} \frac{x^n}{n!} \sum_{k=1}^{n} S(n,k) a_k \\ &= \sum_{k\geq 1} a_k \sum_{n\geq k} \frac{S(n,k)x^n}{n!} \\ &= \sum_{k\geq 1} \frac{a_k(\exp(x)-1)^k}{k!} \\ &= A(\exp(x)-1), \end{aligned}$$

by Lemma 8.

The converse is proved by reversing the argument.

Corollary 10 *The exponential generating function for the Bell numbers is*

$$\sum_{n\geq 0} \frac{B(n)x^n}{n!} = \exp(\exp(x)-1).$$

Proof Apply Proposition 9 to the sequence with $a_n = 1$ for all n; or sum the equation of Lemma 8 over k.

Number partitions

The partition number $p(n)$ is the number of partitions of an n-set, up to permutations of the set.

The key to evaluating $p(n)$ is its generating function:

$$\sum_{n\geq 0} p(n)x^n = \left(\prod_{k\geq 1}(1-x^k)\right)^{-1}.$$

For $(1-x^k)^{-1} = 1+x^k+x^{2k}+\cdots$. Thus a term in x^n in the product, with coefficient 1, arises from every expression $n = \sum c_k k$, where the c_k are non-negative integers, all but finitely many equal to zero. This number is $p(n)$, since we can regard $n = \sum c_k k$ as an alternative expression for a partition of n.

We will use this in the next chapter to give a recurrence relation for $p(n)$.

Permutations

A permutation of $\{1,\ldots,n\}$ is a bijective function from this set to itself.

In the nineteenth century, a more logical terminology was used. Such a function was called a substitution, while a permutation was a sequence $(a_1, a_2, \ldots, a_n)$ containing each element of the set precisely once. Since there is a natural ordering of $\{1, 2, \ldots, n\}$, there is a one-to-one correspondence between "permutations" and "substitutions": the sequence $(a_1, a_2, \ldots, a_n)$ corresponds to the function $\pi : i \mapsto a_i$, for $i = 1, \ldots, n$.

The correspondence between permutations and total orderings of an n-set has profound consequences for a number of enumeration problems. For now we return to the usage "permutation = bijective function". We refer to the sequence $(a_1, \ldots, a_n)$ as the *passive form* of the permutation π in the last paragraph; the function is the *active form* of the permutation.

Following the conventions of algebra, we write a permutation on the right of its argument, so that $i\pi$ is the image of i under the permutation π (that is, the ith term of the passive form of π).

The set of permutations of $\{1, \ldots, n\}$, with the operation of composition, is a group, called the *symmetric group* S_n. Products, identity, and inverses of permutations always refer to the operations in this group.

Unlabelled permutations

As for partitions, we can consider unlabelled or labelled permutations, that is, permutations of an n-set or equivalence classes of permutations. We dispose of unlabelled permutations first.

Two permutations π_1 and π_2 of $\{1, \ldots, n\}$ are equivalent if there is a bijection σ of $\{1, \ldots, n\}$ (that is, a permutation!) such that, for all $i \in \{1, \ldots, n\}$, we have

$$(i\sigma)\pi_2 = j\sigma \quad \text{if and only if} \quad i\pi_1 = j,$$

in other words, $i\sigma\pi_2 = i\pi_1\sigma$ for all i, so that $\pi_2 = \sigma^{-1}\pi_1\sigma$. Thus, this equivalence relation is the algebraic relation of *conjugacy* in the symmetric group; the unlabelled permutations are conjugacy classes of S_n..

Now recall the *cycle decomposition* of permutations:

> Any permutation of a finite set can be written as the disjoint union of cycles, uniquely up to the order of the factors and the choices of starting points of the cycles.

Moreover,

> Two permutations are equivalent if and only if the lists of cycle lengths of the two permutations (written in non-increasing order) are equal.

Thus equivalence classes of permutations correspond to partitions of the integer n. This means that the enumeration theory for "unlabelled permutations" is the same as that for "unlabelled partitions", discussed in the last section.

Labelled permutations

The *parity* of a permutation π of $\{1,\ldots,n\}$ is defined as the parity of $n-k$, where k is the number of cycles of π (in its decomposition as a product of distinct cycles). The *sign* of π is $(-1)^p$, where p is the parity of π.

Parity and sign have various important algebraic properties. For example,

- the parity of π is equal to the parity of the number of factors in any expression for π as a product of disjoint cycles;
- parity is a homomorphism from the symmetric group S_n to the group $\mathbb{Z}/(2)$ of integers mod 2, and hence sign is a homomorphism to the multiplicative group $\{\pm 1\}$.
- For $n > 1$, these homomorphisms are onto; their kernel (the set of permutations of even parity, or of sign $+1$) is a normal subgroup of index 2 in S_n, called the *alternating group* A_n.

The *Stirling numbers of the first kind* are defined by the rule that $s(n,k)$ is $(-1)^{n-k}$ times the number of permutations of $\{1,\ldots,n\}$ having k cycles. Sometimes the number of such permutations is referred to as the *unsigned Stirling number*.

Clearly we have

$$\sum_{k=1}^{n} |s(n,k)| = n!\,.$$

Slightly less obviously,

$$\sum_{k=1}^{n} s(n,k) = 0$$

for $n > 1$. The algebraic proof of this depends on the fact that sign is a homomorphism to $\{\pm 1\}$, so that the two values are taken equally often. We will see a combinatorial proof later.

Proposition 11 *The recurrence relation for the Stirling numbers is*

$$s(n,1) = (-1)^{n-1}(n-1)!, \quad s(n,n) = 1,$$
$$s(n,k) = s(n-1,k-1) - (n-1)s(n-1,k) \text{ for } 1 < k < n.$$

Proof We split the permutations into two classes: those for which (n) is a single part (obtained by adjoining this cycle to a permutation of $\{1,\ldots,n-1\}$ with $k-1$ cycles), and the remainder (obtained by taking a permutation of $\{1,\ldots,n-1\}$ with k cycles and interpolating n at some position in one of the cycles). The second construction, but not the first, changes the sign of the permutations.

To see that there are $(n-1)!$ permutations with a single cycle, note that if we choose to start the cycle with 1 then the remaining $n-1$ elements can be written into the cycle in any order.

Note that, if we instead define $s(n,0)$ and $s(n,n+1)$ to be equal to 0 for $n \geq 1$, then the recurrence holds also for $k=1$ and $k=n$. We use this below.

The generating function is given by the following result:

Proposition 12 $\sum_{k=1}^{n} s(n,k)x^k = (x)_n$.

Proof The result is clear for $n=1$, Suppose that it holds for $n=m-1$.

$$\begin{aligned}\sum_{k=1}^{m} s(m,k)x^k &= \sum_{k=1}^{m} s(m-1,k-1)x^k - \sum_{k=1}^{m}(m-1)s(m-1,k)x^k \\ &= (x-m+1)(x)_{m-1} \\ &= (x)_m.\end{aligned}$$

Note that substituting $x=1$ into this equation shows that $\sum_k s(n,k)=0$ for $n \geq 2$.

Corollary 13 *The triangular matrices S_1 and S_2 whose entries are the Stirling numbers of the first and second kinds are inverses of each other.*

Proof Propositions 7 and 12 show that S_1 and S_2 are the transition matrices between the bases $(x^n : n \geq 1)$ and $((x)_n\ n \geq 1)$ of the space of real polynomials with constant term zero.

Proposition 14 *Let $(a_0,a_1,\ldots)$ and $(b_0,b_1,\ldots)$ be two sequences of numbers, with exponential generating functions $A(x)$ and $B(x)$ respectively. Then the following two conditions are equivalent:*

(a) $b_0 = a_0$ and $b_n = \sum_{k=1}^{n} s(n,k)a_k$ for $n \geq 1$;

(b) $B(x) = A(\log(1+x))$.

Proof This is the "inverse" of Proposition 9.

We have counted permutations by number of cycles. A more refined count is by the list of cycle lengths.

Let $c_k(\pi)$ be the number of k-cycles in the cycle decomposition of π.

Proposition 15 *The size of the conjugacy class of π in S_n is*

$$\frac{n!}{\prod_k k^{c_k(\pi)} c_k(\pi)!}.$$

Proof Write out the pattern for the cycle structure of a permutation with $c_k(\pi)$ cycles of length k for all k, leaving blank the entries in the cycles. There are $n!$ ways of entering the numbers $1,\ldots,n$ in the pattern. However, each cycle of length k can be written in k different ways, since the cycle can start at any point; and the cycles of length k can be written in any of the $c_k(\pi)!$ possible orders. So the number of ways of entering the numbers $1,\ldots,n$ giving rise to each permutation in the conjugacy class is $\prod k^{c_k(\pi)} c_k(\pi)!$.

The *cycle index* of the symmetric group S_n is the generating function for the numbers $c_k(\pi)$, for $k = 1,\ldots,n$. By convention it is normalised by dividing by $n!$. Thus,

$$Z(S_n) = \sum_{\pi\in S_n} \prod_{k=1}^{n} s_k^{c_k(\pi)}.$$

Because of the normalisation, this can be thought of as the probability generating function for the cycle structure of a random permutation: that is, the coefficient of the monomial $\prod s_k^{a_k}$ (where $\sum kc_k = n$) is the probability that a random permutation π has $c_k(\pi) = a_k$ for $k = 1,\ldots,n$ — this is

$$\frac{1}{\prod_k k^{a_k} a_k!}.$$

One result which we will meet later is the following. We adopt the convention that $Z(S_0) = 1$.

Proposition 16 $\displaystyle\sum_{n\geq 0} Z(S_n) = \exp\left(\sum_{k\geq 1} \frac{s_k}{k}\right).$

Proof The left-hand side is equal to

$$\sum_{n\geq 0} \sum_{\sum a_k = n} \prod_{k\geq 1} \frac{s_k^{a_k}}{k^{a_k} a_k!} \quad = \quad \sum_{a_1,a_2,\ldots} \prod_{k\geq 1} \frac{s_k^{a_k}}{k^{a_k} a_k!}$$

$$
\begin{aligned}
&= \prod_{k\geq 1} \sum_{a\geq 0} \frac{s_k^a}{k^a a!} \\
&= \prod_{k\geq 1} \exp\left(\frac{s_k}{k}\right) \\
&= \exp\left(\sum_{k\geq 1} \frac{s_k}{k}\right)
\end{aligned}
$$

as required. (The sum on the right-hand side of the first line is over all infinite sequences of natural numbers $(a_1, a_2, \ldots)$ with only finitely many entries non-zero.)

We will see much more about cycle index in the chapter on orbit counting.